An Elementary and Simple Proof of Fermat's Last Theorem

Mike Winkler
Fakultät für Mathematik, Ruhr-Universität Bochum
mike.winkler@ruhr-uni-bochum.de
www.mikewinkler.co.nf

March 19, 2018

Abstract

Fermat's Last Theorem states that the Diophantine equation $X^n + Y^n = Z^n$ has no non-trivial solution for any n greater than 2. In this paper we give a brief and simple proof of the theorem using only elementary methods.

Introduction

The only known successful proof of Fermat's Last Theorem was given in 1994 by Andrew Wiles [5]. Unfortunately this proof contains nearly hundred pages and can be understood in its entirety only by some specialists. For this reason and relating to Fermat's famous marginal note[1], many people (mostly amateurs) are still looking for a shorter and simpler proof based on elementary methods. In this paper we present such a proof.

To prove Fermat's Last Theorem it suffices to prove it for the exponent 4 and every odd prime exponent. A proof for the case $n = 4$ has already been given by Fermat himself. Therefore we give our proof only for the prime exponents greater than 2. First, we proof the correctness of the Diophantine identity $(z - y)^n = z^n - y^n - nzy(z-y)\lambda_{n,y,z}$ with $gcd(y, z, \lambda_{n,y,z}) = 1$ for any odd prime n. Then we use the identity $z^n = axy - b(x + y) + c$ with $a, b, c \in \mathbb{Z}$ to convert the equation $x^n + y^n = z^n$ to the form $bx^{n+1} + b(z^{n+1} - y^{n+1}) = cx^n + ax(z^{n+1} - y^{n+1})$. Finally, we show that x^n must divide $(z^{n+1} - y^{n+1})$. From this we deduce that $x^n + y^n = z^n$ holds only for the trivial solutions.

[1] See [4] for the complete text.

The Proof

Lemma 1. *Let p, q be integers with $gcd(p, q) = 1$. Then for any odd prime n there exists an integer $\lambda_{n,p,q}$ with $gcd(p, q, \lambda_{n,p,q}) = 1$ such that*

$$(p-q)^n = p^n - q^n - npq(p-q)\lambda_{n,p,q}. \tag{1}$$

Proof. According to the binomial theorem, we have

$$\begin{aligned}(p-q)^n &= \sum_{k=0}^{n} \binom{n}{k} p^{n-k}(-q)^k \\ &= p^n - q^n + \sum_{k=1}^{n-1} \binom{n}{k} p^{n-k}(-q)^k \\ &= p^n - q^n - npq \cdot \sum_{k=1}^{n-1} \frac{1}{n}\binom{n}{k} p^{n-k-1}(-q)^{k-1} \\ &= p^n - q^n - npq(p-q) \cdot \sum_{k=1}^{n-2} \frac{1}{n}\left(\binom{n-1}{k} + (-1)^{k+1}\right) p^{n-k-2}(-q)^{k-1}. \end{aligned} \tag{2}$$

The term $\frac{1}{n}\left(\binom{n-1}{k} + (-1)^{k+1}\right)$ assumes only positive integer values for and odd prime n. A proof can be found in Mamakani [2]. The OEIS reference for these values is A219539 [3].

By substituting $\lambda_{n,p,q} = \sum_{k=1}^{n-2} \frac{1}{n}\left(\binom{n-1}{k} + (-1)^{k+1}\right) p^{n-k-2}q^{k-1}$ into (2) we get (1). For $n = 3$ we have $\lambda_{3,p,q} = 1$. For primes $n > 3$ it follows from $gcd(p, q) = 1$ and the expansion of $\lambda_{n,p,q}$, given by

$$p^{n-3} - \frac{\binom{n-1}{2} - 1}{n} p^{n-4}q + \cdots - \frac{\binom{n-1}{n-3} - 1}{n} pq^{n-4} + q^{n-3}, \tag{3}$$

that $gcd(p, q, \lambda_{n,p,q}) = 1$. Because if p divides $\lambda_{n,p,q}$ then $p \mid q^{n-3}$, and if q divides $\lambda_{n,p,q}$ then $q \mid p^{n-3}$. This completes the proof. □

Lemma 2. *Let a, b, c be integers defined by*

$$a = \frac{1}{z-y} \cdot \sum_{k=0}^{n-2} x^{n-2-k}(z^{k+1} - y^{k+1}), \tag{4}$$

$$b = \frac{1}{z-y} \cdot \sum_{k=0}^{n-1} x^{n-1-k}(z^{k+1} - y^{k+1}), \tag{5}$$

$$c = \frac{1}{z-y} \cdot \sum_{k=0}^{n} x^{n-k}(z^{k+1} - y^{k+1}), \tag{6}$$

then the identity

$$z^n = axy - b(x+y) + c, \tag{7}$$

holds for all integers x, y, z and any nonnegative integer n.

Proof. Multiplying (4) by x gives

$$ax = \frac{1}{z-y} \cdot \sum_{k=0}^{n-2} x^{n-1-k}(z^{k+1} - y^{k+1}).$$

Adding $\frac{z^n-y^n}{z-y}$ we get

$$ax + \frac{z^n - y^n}{z-y} = \frac{1}{z-y} \cdot \sum_{k=0}^{n-1} x^{n-1-k}(z^{k+1} - y^{k+1}) = b.$$

Multiplying by $(z-y)$ yields

$$ax(z-y) + z^n - y^n = b(z-y). \tag{8}$$

Multiplying (5) by x we have

$$bx = \frac{1}{z-y} \cdot \sum_{k=0}^{n-1} x^{n-k}(z^{k+1} - y^{k+1}).$$

Adding $\frac{z^{n+1}-y^{n+1}}{z-y}$ we get

$$bx + \frac{z^{n+1} - y^{n+1}}{z-y} = \frac{1}{z-y} \cdot \sum_{k=0}^{n} x^{n-k}(z^{k+1} - y^{k+1}) = c.$$

Multiplying by $(z-y)$ we obtain

$$bx(z-y) + z^{n+1} - y^{n+1} = c(z-y). \tag{9}$$

Now we can prove the evidence of (7). Multiplying (7) by $(z-y)$ gives

$$z^n(z-y) = axy(z-y) - b(x+y)(z-y) + c(z-y).$$

Applying (8) on the right-hand side we get

$$\begin{aligned} z^n(z-y) &= y\big(b(z-y) - z^n + y^n\big) - b(x+y)(z-y) + c(z-y) \\ &= -bx(z-y) - yz^n + y^{n+1} + c(z-y). \end{aligned}$$

Applying (9) on the right-hand side yields

$$\begin{aligned} z^n(z-y) &= -bx(z-y) - yz^n + y^{n+1} + bx(z-y) + z^{n+1} - y^{n+1} \\ &= z^{n+1} - yz^n. \end{aligned}$$

We obtain a true statement, which completes the proof. □

Lemma 3. *Let x, y, z be nonzero integers with $gcd(x, y, z) = 1$ and let n be an odd prime. According to Lemma 2, if $n \nmid x$ and $(z-y) \mid x$, we have $gcd(x, b) = 1$.*

Proof. Let p_x be a prime factor of $(z-y)$ and x. For $k = 0, \ldots, n-2$ we have

$$\frac{z^{k+1} - y^{k+1}}{z-y} = \sum_{i=0}^{k} z^{k-i}y^i.$$

Thus it follows from (5) that only $\frac{z^n-y^n}{z-y}$ decides whether p_x divides b, because its the only term in the sum without the factor x. Applying Lemma 1 with $p = z$, $q = y$, we obtain

$$\frac{z^n - y^n}{z - y} = (z - y)^{n-1} + nzy\lambda_{n,z,y}, \tag{10}$$

with $gcd(z, y, \lambda_{n,z,y}) = 1$. Because x, y, z are pairwise relatively prime, exactly one of these integers is even. If x is even then y, z are odd, so $(z-y)$ is even. Applying Lemma 1 it follows from (3) that $\lambda_{n,z,y}$ is odd, because the sum consists of an odd number of terms, where the number of even coefficients is also even and the number of odd coefficients is also odd. If x is odd then y, z have different parity, so $(z - y)$ is odd. Applying Lemma 1 it follows from (3) that $\lambda_{n,z,y}$ is odd, because each term in the sum is even except $(z^{n-3}+y^{n-3})$ which is odd. From $gcd(z, y) = 1$ we have $gcd(z, y, z-y) = 1$, hence $gcd(z - y, \lambda_{n,z,y}) = 1$, so $gcd(z - y, zy\lambda_{n,z,y}) = 1$. It follows with $(z - y) \mid x$, $n \nmid x$ and $x \neq \pm 1$ that $p_x \nmid nzy\lambda_{n,z,y}$. Hence p_x does not divide the right-hand side of (10), which completes the proof. □

Theorem 4. *The Diophantine equation $X^n + Y^n = Z^n$ has no non-trivial solution for any odd prime number n.*

Proof. We assume that x, y, z are nonzero integers and n is an odd prime such that

$$x^n + y^n = z^n. \tag{11}$$

It suffices to consider only solutions (x, y, z) with $gcd(x, y, z) = 1$. Hence x, y, z are pairwise relatively prime and exactly one of these integers is even. Applying Lemma 1 with $p = x + y$, $q = z$, we have

$$(x + y - z)^n = (x + y)^n - z^n - n(x + y)z(x + y - z)\lambda_{n,x+y,z}.$$

Applying Lemma 1 with $p = x$, $q = -y$, on the right-hand side gives

$$(x + y - z)^n = x^n + y^n + nxy(x + y)\lambda_{n,x,-y} - z^n - n(x + y)z(x + y - z)\lambda_{n,x+y,z}.$$

Applying (11) on the right-hand side we obtain

$$(x + y - z)^n = nxy(x + y)\lambda_{n,x,-y} - n(x + y)z(x + y - z)\lambda_{n,x+y,z},$$

that is

$$(x + y - z)^n = n(x + y)\big(xy\lambda_{n,x,-y} - z(x + y - z)\lambda_{n,x+y,z}\big). \tag{12}$$

Because n is an odd prime we conclude from (12) that $n \mid (x+y-z)^n$, hence $n \mid (x+y-z)$. From $gcd(x, y, z) = 1$ it follows that n divides one and only one of the integers x, y, z. Applying (11) on the right-hand side of (8) we obtain

$$ax(z - y) + x^n = b(z - y),$$

hence

$$x^n = (b - ax)(z - y). \tag{13}$$

From (9) we have

$$z^{n+1} - y^{n+1} = (c - bx)(z - y). \tag{14}$$

Combining (13) with (14) yields

$$x^n(c - bx) = (z^{n+1} - y^{n+1})(b - ax),$$

that is

$$bx^{n+1} + b(z^{n+1} - y^{n+1}) = cx^n + ax(z^{n+1} - y^{n+1}). \tag{15}$$

Now we assume that $x \neq \pm 1$ and $n \nmid x$. Applying Lemma 1 with $p = z$, $q = y$, it follows from (11) that $(z - y) \mid x^n$. From $gcd(x, y, z) = 1$ and $gcd(z, y, \lambda_{n,z,y}) = 1$ we have $gcd(z - y, \lambda_{n,z,y}) = 1$, and so $(z - y) \mid x$. By Lemma (3) we have $gcd(x, b) = 1$. Hence, dividing (15) by x we obtain

$$bx^n + b \cdot \frac{z^{n+1} - y^{n+1}}{x} = cx^{n-1} + a(z^{n+1} - y^{n+1}),$$

which gives $x \mid (z^{n+1} - y^{n+1})$. Hence x divides the right-hand side, so

$$bx^{n-1} + b \cdot \frac{z^{n+1} - y^{n+1}}{x^2} = cx^{n-2} + a \cdot \frac{z^{n+1} - y^{n+1}}{x},$$

and consequently $x^2 \mid (z^{n+1} - y^{n+1})$. Thus it follows that (15) can be divide n times by x, which yields

$$bx + b \cdot \frac{z^{n+1} - y^{n+1}}{x^n} = c + a \cdot \frac{z^{n+1} - y^{n+1}}{x^{n-1}}. \tag{16}$$

Multiplying (11) by z gives

$$zx^n + zy^n = z^{n+1}.$$

Subtracting y^{n+1} we obtain

$$zx^n + y^n(z - y) = z^{n+1} - y^{n+1}.$$

Dividing by x^n yields

$$z + \frac{y^n(z - y)}{x^n} = \frac{z^{n+1} - y^{n+1}}{x^n}. \tag{17}$$

From (16) we conclude that $x^n \mid (z^{n+1} - y^{n+1})$. Hence, from (17) it follows with $gcd(x, y, z) = 1$ that $x^n \mid (z - y)$. This clearly forces with $(z - y) \mid x$ that $x = \pm 1$, which is a contradiction to our assumption $x \neq \pm 1$. Hence, a non-trivial solution with $n \nmid x$ can not exists. In the case $n \mid x$ we can interchange x and y, which completes the proof. □

Remark 5. The terms from (4)–(6) represent special cases of the trinomial expansion of $(x + y + z)^n$ with the peculiarity that all trinomial coefficients given by $\binom{n}{i,j,k} = \frac{n!}{i!\,j!\,k!}$ were set equal to 1. Let x, y, z be integers, then for any nonnegative integer n we have

$$\frac{1}{z - y} \cdot \sum_{k=0}^{n} x^{n-k}(z^{k+1} - y^{k+1}) = \sum_{i+j+k=n} x^i y^j z^k,$$

where i, j, k are all nonnegative integers such that $i + j + k = n$.

Remark 6. We can rewrite the terms from (4)–(6) as fractions. From (4) we obtain

$$a = \frac{z}{z-y} \cdot \sum_{k=0}^{n-2} x^{n-2-k} z^k - \frac{y}{z-y} \cdot \sum_{k=0}^{n-2} x^{n-2-k} y^k$$

$$= \frac{z}{z-y} \cdot \frac{z^{n-1} - x^{n-1}}{z-x} - \frac{y}{z-y} \cdot \frac{y^{n-1} - x^{n-1}}{y-x}$$

$$= \frac{x^n(z-y) + y^n(x-z) + z^n(y-x)}{(z-y)(x-z)(x-y)}$$

$$= \frac{x^n(z-y) + y^n(x-z) + z^n(y-x)}{x^2(z-y) + y^2(x-z) + z^2(y-x)}.$$

In a similar way, we may show that

$$b = \frac{x^{n+1}(z-y) + y^{n+1}(x-z) + z^{n+1}(y-x)}{x^2(z-y) + y^2(x-z) + z^2(y-x)},$$

$$c = \frac{x^{n+2}(z-y) + y^{n+2}(x-z) + z^{n+2}(y-x)}{x^2(z-y) + y^2(x-z) + z^2(y-x)}.$$

Table 1 gives an overview on all possible integer values for a, b, c from (4)–(6) for any nonnegative integer n.

n	a	b	c
0	0	0	1
1	0	1	$\in \mathbb{Z}$
2	1	$\in \mathbb{Z}$	$\in \mathbb{N}$
odd ≥ 3	$\in \mathbb{Z}$	$\in \mathbb{N}$	$\in \mathbb{Z}$
even ≥ 4	$\in \mathbb{N}$	$\in \mathbb{Z}$	$\in \mathbb{N}$

Table 1: Possible values for a, b, c.

Acknowledgements

The author wishes to express his thanks to Andreas Fillipi. Without his contribution in a mathematics forum, I probably would never have worked on this topic again [1].

References

[1] Fillipi, Andreas: *Beitrag im Forum Elementare Zahlentheorie*, February 9, 2015, www.matheplanet.de. (tinyurl.com/y8jh4dvr)

[2] K. Mamakani, F. Ruskey, *New roses: simple symmetric Venn diagrams with 11 and 13 curves*, Disc. Comp. Geom., 52 (2014), pp. 71–87, Lemma 2.

[3] The On-Line Encyclopedia of Integer Sequences: *T(n,k) is the number of k-points on the left side of a crosscut of simple symmetric n-Venn diagram*, A219539.

[4] Wikipedia, *Fermat's Last Theorem*, 2.2 Fermat's conjecture. (tinyurl.com/y9hwwdb5)

[5] Wiles, Andrew: *Modular Elliptic Curves and Fermat's last theorem*, Annals of Mathematics 142 (1995), pp. 443-551.